ТРАНСПОРТНЫЕ СИСТЕМЫ
2.9.1 – Транспортные и транспортно-технологические системы страны, ее регионов и городов, организация производства на транспорте;
2.9.4. – Управление процессами перевозок;
2.9.6 – Аэронавигация и эксплуатация авиационной техники;
2.9.8 – Интеллектуальные транспортные системы

УДК 621.396.96:621.396
DOI: 10.26467/2079-0619-2025-28-6-8-24

Методика повышения помехоустойчивости приемника спутниковой навигации к воздействию преднамеренных помех

Р.О. Арефьев[1], Н.Г. Арефьева[1], О.Н. Скрыпник[2]
[1]Иркутский филиал Московского государственного технического университета гражданской авиации, г. Иркутск, Россия
[2]Белорусская государственная академия авиации, г. Минск, Республика Беларусь

Аннотация: Современные беспилотные воздушные суда (БВС) оснащены приемниками спутниковой навигации для решения задач стабилизации в пространстве и выдерживания заданной траектории полета. При этом приемники спутниковой навигации отличаются низкой помехоустойчивостью, что может привести к потере сигналов от спутников и, как следствие, к отклонению БВС от заданного маршрута либо к потере управляемости. В данной работе представлена методика повышения помехоустойчивости приемника спутниковой навигации при воздействии широкополосной и узкополосной помех, а также уводящей помехи. Методика реализована на основе анализа выходных данных с приемника спутниковой навигации, формируемых в формате NMEA. Основным достоинством предлагаемого подхода является использование относительно небольших вычислительных ресурсов бортового вычислителя. Предлагаемая методика основана на анализе соотношения сигнал/шум, количества навигационных спутников, используемых в решении навигационной задачи, а также на целостности выходных координат приемника БВС. На основе предложенной методики разработан алгоритм обнаружения воздействия помех, который состоит из двух этапов. На первом этапе определяется наличие помех, второй этап предполагает анализ выходных координат приемника по отношению к планируемым, что позволяет определить воздействия уводящей помехи. Алгоритм реализован на языке программирования G в программной среде LabVIEW. Методика и алгоритм обнаружения помех протестированы путем проведения ряда полунатурных экспериментов с помощью имитатора сигналов СН-3803М, что позволило оценить пороговые значения уровней сигналов от навигационных спутников при наличии помех. В качестве тестируемого образца использовался мультисистемный приемник спутниковой навигации ATGM336H, который обладает возможностью выбора спутниковой навигационной системы (ГЛОНАСС, GPS или BeiDou) или их комбинации для решения задачи навигации БВС. Проведена серия экспериментов по оценке влияния помех различных видов на характеристики приемника спутниковой навигации ATGM336H.

Ключевые слова: БВС, спуфинг, GNSS, соотношение сигнал/шум, NMEA, помехоустойчивость.

Для цитирования: Арефьев Р.О., Арефьева Н.Г., Скрыпник О.Н. Методика повышения помехоустойчивости приемника спутниковой навигации к воздействию преднамеренных помех // Научный вестник МГТУ ГА. 2025. Т. 28, № 6. С. 8–24. DOI: 10.26467/2079-0619-2025-28-6-8-24

Technique for improving the immunity of a satellite navigation receiver to intended jamming

R.O. Arefyev[1], N.G. Arefyeva[1], O.N. Skrypnik[2]
[1]Irkutsk branch of the Moscow State Technical University of Civil Aviation, Irkutsk, Russia
[2]Belarusian State Aviation Academy, Minsk, Republic of Belarus

Abstract: Modern unmanned air vehicles (UAV) are equipped with satellite navigation receivers to provide stability in space and maintain the desired track. The satellite navigation receivers feature low noise immunity that can result in loss of satellite signals

and, hence, in deviation from the desired track or control loss. The paper presents a technique for improving the immunity of a satellite navigation receiver under wide- and narrow-band interference as well as deceptive interference. The technique was implemented through the analysis of NMEA output data of a satellite navigation receiver. The main advantage of the proposed technique is the use of relatively small computational power of the onboard computer. The proposed technique is based on the analysis of the signal/noise ratio, the number of navigation satellites used as well as the integrity of the output coordinates of an UAV receiver. The proposed technique allowed developing an algorithm for detecting the interference which consists of two stages. At the first stage, presence of interference is identified, the second stage implies the comparison of the output coordinates of the receiver with the desired ones making it possible to assess the effects of deceptive interference. The algorithm is implemented in the G programming language in the LabVIEW environment. The technique and the algorithm for identifying the interference were tested by conducting a series of semi-natural experiments with the CH-3803M signal simulator which allowed estimating the threshold values of signal levels from navigation satellites in the presence of interference. As a test sample the ATGM336H multisystem satellite navigation receiver was used that provides a possibility to select a satellite navigation system (GLONASS, GPS or BeiDou) or to use their combination for solving an UAV navigation problem. The authors conducted a series of experiments for assessing the effects of different interference on the performance of the ATGM336H satellite navigation receiver.

Key words: UAV, spoofing, GNSS, signal/noise ratio, NMEA, noise immunity.

For citation: Arefyev, R.O., Arefyeva, N.G., Skrypnik, O.N. (2025). Technique for improving the immunity of a satellite navigation receiver to intended jamming. Civil Aviation High Technologies, vol. 28, no. 6, pp. 8–24. DOI: 10.26467/2079-0619-2025-28-6-8-24

Введение

Беспилотные авиационные системы (БАС) являются динамически развивающимся кластером авиационной отрасли. Области использования беспилотных воздушных судов (БВС) обширны, и постоянно находятся новые направления их применения. При этом в перспективе предполагается все более широкое применение БВС при осуществлении ими автономных полетов.

Возможность и эффективность выполнения автономных полетов БВС зависит от качества и надежности аэронавигационного обеспечения. В качестве основного средства для осуществления автономного полета используются спутниковые навигационные системы (GNSS), которые обладают глобальной рабочей зоной, высокой точностью, неограниченной пропускной способностью. Однако существует и ряд проблем [1–9], которые влияют на эффективность использования спутниковой навигации, наиболее значимой из которых является слабая помехоустойчивость GNSS-приемников. Это связано с тем, что сигналы от навигационных спутников (НС) на входе приемной антенны имеют весьма низкий уровень и достаточно небольшого уровня внешней помехи для того, чтобы подавить слабые сигналы от НС. При этом существуют преднамеренные помехи, имитирующие структуру сигналов от НС, которые могут привести к определению приемником ложных координат и формированию ложных траекторий полета БВС, что делает использование воздушного пространства небезопасным для других пользователей. Помехи такого рода называются уводящими помехами, а подмена сигналов GNSS – спуфингом (от английского spoof – подмена, обман, подделка) [10–13]. В работе [14] проведен анализ статистических данных за 2024 год, показывающий рост случаев спуфинга при выполнении регулярных полетов пилотируемой авиацией. Поэтому возникает актуальная научная задача по определению наличия спуфинга и противодействию ему, что позволит повысить безопасность полетов и эффективность аэронавигационного обеспечения пилотируемой и беспилотной авиации.

Основными сценариями спуфинга являются следующие:

использование постановщика помех для того, чтобы вывести приемник GNSS из режима слежения в режим поиска и захвата сигналов GNSS, и после обнуления коррелятора подать на вход приемника ложный спутниковый сигнал для формирования ложной траектории. Такой сценарий рассматривается как грубый вид спуфинга;

использование на постановщике помехи приемника GNSS для получения идентичных задержек сигналов и значений доплеровских сдвигов частоты, необходимых для формиро-

вания синхронного спуфинга с бóльшим уровнем сигнала по сравнению с уровнями сигналов от НС, что позволит сделать подмену на ложный сигнал. Такой вид спуфинга является более сложным и труднее обнаруживаемым.

Согласно работам [15, 16] существуют следующие методы обнаружения спуфинга:

- определение амплитуды сигнала;
- определение направления прихода сигнала;
- определение времени поступления сигнала;
- сопоставление данных приемника GNSS с данными других бортовых навигационных систем;
- аутентификация с использованием шифрования сигнала;
- определение вида поляризации сигнала;
- обнаружение контуров векторного слежения.

Для того чтобы использовать любой из рассмотренных методов, необходимо знать структуру конкретных приемников GNSS и реализуемых в них алгоритмов поиска, обнаружения сигналов НС и слежения за их задержкой и частотой. На практике большинство приемников GNSS, устанавливаемых на БВС, являются отдельными модулями с закрытой структурой, что ограничивает использование большинства из указанных методов обнаружения спуфинга.

В работе [2] проведена оценка помехоустойчивости мультисистемного приемного модуля GNSS типа ATGM336H в условиях воздействия узкополосных помех. Структура данного приемного модуля позволяет проводить раздельную обработку сигналов по каждой из систем. Экспериментальным путем установлено, что при наличии помехи на частоте GPS ухудшается работа модуля и по системе ГЛОНАСС из-за особенностей выбора промежуточных частот в приемном тракте.

Модуль GNSS, подключенный к бортовому котроллеру БВС, выдает пакет данных с координатами для стабилизации БВС в пространстве и выполнения заданного полета. Однако в случае приема ложных сигналов GNSS, БВС будет выполнять полет не по заданному маршруту, что может быть обнаружено оператором (внешним пилотом) со значительной задержкой. Поэтому необходимо определить момент начала спуфинга и его воздействия на приемник GNSS, чтобы своевременно оповестить оператора для принятия решения по дальнейшему управлению полетом и исключения из контура управления информации, поступающей со спутникового приемника. Для этого предлагается доработка в архитектуре БВС, которая основана на анализе выходных данных со спутникового приемника. Эту задачу может выполнять полетный контроллер при достаточной вычислительной производительности, либо необходим дополнительный микроконтроллер.

В данной работе представлена методика обнаружения спуфинга, формируемого по двум сценариям, рассмотренным выше, которая основана на анализе выходных данных от приемного модуля ATGM336H.

Выходные данные приемного модуля ATGM336H

ATGM336H представляет собой компактный спутниковый приемник, предназначенный для определения координат потребителя, скорости и точного времени UTC при работе по сигналам от систем GPS, ГЛОНАСС и BeiDou. Основные особенности приемного модуля следующие.

1. Поддержка UART-интерфейса для обмена данными и конфигурации.
2. Поддержка высокой скорости передачи данных (до 11 5200 бод).
3. Низкое энергопотребление.
4. Компактный размер, что обеспечивает легкую интеграцию в различные устройства.
5. Встроенная активная антенна.
6. Высокоточное позиционирование (до сантиметрового уровня) с использованием дополнительных технологий.

Приемный модуль ATGM336H имеет ряд характеристик, которые делают его применимым и эффективным в различных областях, включая навигацию БВС.

Выходными данными с приемника является пакет данных в формате NMEA0183.

«NMEA – это общий стандарт представления навигационных данных в текстовом формате (ASCII). Этот протокол используется для передачи ГНСС-данных приемника на внешние устройства, не способные расшифровать навигационное сообщение конкретного производителя приемника»[1].

NMEA-протокол определяет стандартный формат данных, который включает в себя информацию о географическом положении, скорости, времени, курсе и других параметрах полета. Эти данные передаются в виде текстовых сообщений, которые содержат специальные коды и поля для идентификации типа информации.

Для разработки алгоритма обнаружения и парирования спуфинговой атаки предлагается анализировать данные о параметрах принимаемых от НС сигналов, таких как отношение сигнал/шум, азимут и угол места НС, а также информацию о местоположении БВС и параметрах полета. Данную информацию можно получить из протокола NMEA (из сообщений GGA, GSV и RMC). Выбор указанных сообщений обеспечивает полный набор данных приемника и дает полное представление о навигационных условиях.

Проведен анализ публикаций других авторов по использованию данных протокола NMEA для обнаружения спуфинга. Так, в работе [13] рассмотрены существующие методы определения спуфинга, где указывается на возможность анализа данных протокола NMEA. В работе [17] представлены основные сообщения протокола NMEA, которые могут быть использованы для определения спуфинга, приведены результаты тестирования разных типов приемников при наличии спуфинга. В [18] представлена программная платформа для проведения комплексного анализа NMEA-сообщений от двух одновременно работающих приемников, которые расположены на фиксированном расстоянии. Авторами представлены основные методы: проверка навигационных параметров (скорости и высоты); оценка парных расстояний между приемниками; проверка эфемерид; мониторинг смещения шкалы времени; мониторинг соотношения сигнал/шум (определения максимального уровня сигнала). В работе показано, что наиболее эффективным методом определения спуфинга является метод оценки парных расстояний между приемниками для морского транспорта. Метод мониторинга соотношения сигнал/шум в данной работе не использовался.

Структурная схема интерфейса для приемника спутниковой навигации

Для исследования помехозащищенности, оценки точностных характеристик и ряда других задач разработан программный интерфейс приемного модуля ATGM336H. Интерфейс, структурная схема которого представлена на рис. 1, разработан в среде графического программирования LabVIEW.

Приемный модуль ATGM336H подключен к ПЭВМ по последовательному порту RS232 и передает данные в интерфейс с заданной скоростью для дальнейшего преобразования. Из сообщений GSV, GGA, GSA, RMC выделяется соответствующая информация. Так, из сообщения GSV выделяются данные о спутниках, которые находятся в зоне видимости (номер НС, азимут, угол места и соотношение сигнал/шум SNR (Signal to Noise Ration), которое измеряется в дБГц). Из сообщения GGA выделяются координаты, определенные приемным модулем, и время. Далее координаты подвергаются статистической обработке для получения среднеквадратической погрешности (СКО) и графиков ошибок измерения координат. Из сообщения RMC выделяется информация о скорости и курсе движения БВС. В разработанном интерфейсе есть возможность обработки GSA-сообщений для выделения значений геометрического фактора GNSS, который может использоваться для оценки влияния геометрии рабочего созвездия НС на точность измерения координат.

Разработанный интерфейс также позволяет формировать команды в виде сообщения PCAS

[1] Стандарт представления навигационных данных NMEA-0183 [Электронный ресурс] // ОриентСистемс. 2024. URL: https://orsyst.ru/blog/nmea (дата обращения: 23.02.2025).

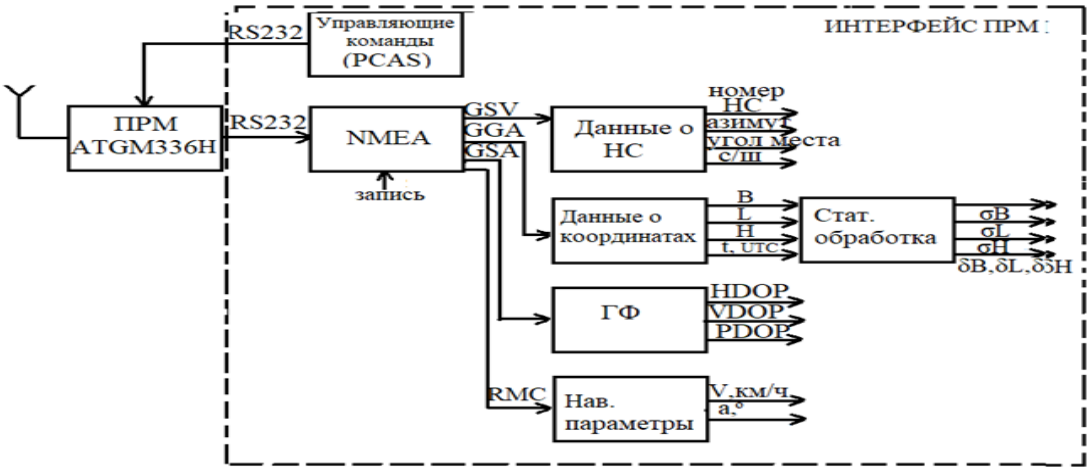


Рис. 1. Интерфейс приемного модуля ATGM336H
Fig. 1. The interface of the ATGM336H receiving module

для изменения настроек приемного модуля. Так, например, с помощью соответствующей команды можно выбрать спутниковую систему (системы), по которой будет осуществляться работа приемного модуля, изменить скорость выдаваемой информации и др.

Полученные и преобразованные данные в дальнейшем анализируются, в результате чего можно изменять конфигурацию приемного модуля с помощью сформированной команды, что может улучшить его работу при наличии помех.

Методика борьбы со спуфингом

Проведенный анализ существующих методов формирования ложных сигналов показывает, что на данный момент наиболее простым способом осуществления спуфинга является использование оборудования HackRF One (программно-управляемая платформа) и внешнего усилителя радиосигналов. С учетом этого методика обнаружения уводящей помехи должна быть обобщенной и включать несколько ключевых критериев обнаружения спуфинга.

Как было отмечено ранее, основным показателем определения спуфинга на борту БВС будет оценка уровней соотношения сигнал/шум, что позволит обнаружить наличие помехи, которая предшествует подменному сигналу. Поэтому еще одним показателем обнаружения спуфингового сигнала будет сравнение бортового плана полета с данными, получаемыми с приемника GNSS. Исходя из этого, методика определения спуфинговой атаки состоит из двух этапов:

1) анализа соотношения сигнал/шум на входе приемника для определения конкретных уровней сигнала, которые могут указывать на наличие помехи;

2) сравнения дополнительной информации, такой как план полета (координаты, курс, скорость), с данными, получаемыми от приемника GNSS, что позволит обнаружить несоответствия и стать основанием для реакции на спуфинг.

Определение пороговых уровней отношения сигнал/шум

Определение пороговых уровней отношения сигнал/шум для обнаружения спуфинга выполнялось с помощью имитатора спутниковых сигналов СН-3803М. Одним из достоинств имитатора является возможность изменения мощности выходного сигнала в диапазоне от −150 до −100 дБмВт. В реальных условиях эксплуатации приемника уровень сигнала соответствует −120 дБмВт [2, 19].

Имитировались сигналы от навигационных спутников ГЛОНАСС и GPS. Антенна приемника устанавливалась рядом с антенной имитатора.

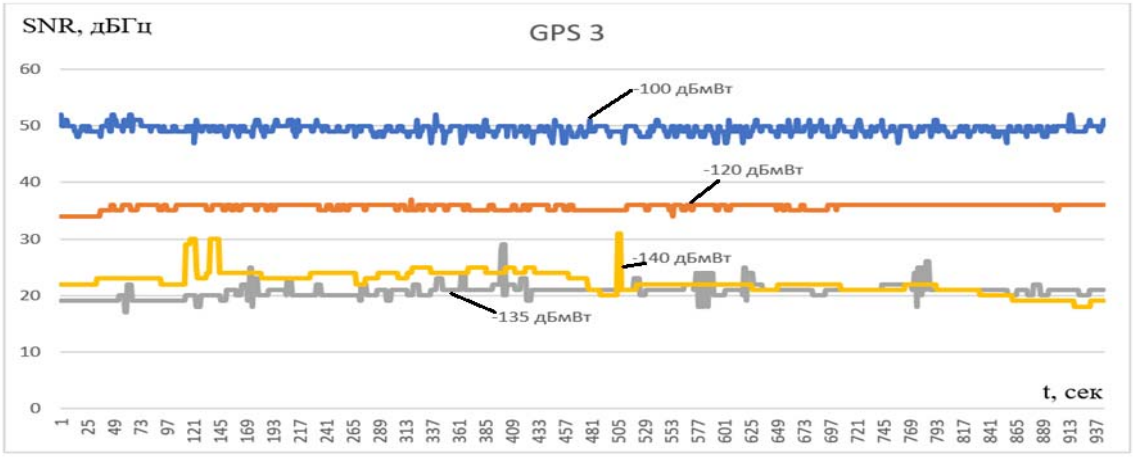


Рис. 2. SNR навигационного спутника GPS № 3 при разных уровнях входного сигнала
Fig. 2. SNR of GPS satellite No. 3 at different input levels

Таблица 1
Table 1

Средние значения SNR для разных уровней входного сигнала
Average SNR values for different input signal levels

Уровень входного сигнала, дБмВт	−100	−120	−135	−140
Среднее SNR GPS, дБГц	50,6	38,8	26,4	24,2
Среднее SNR ГЛОНАСС, дБГц	52	39,6	28,6	23,3

Была проведена серия экспериментов с разными уровнями выходного сигнала от имитатора, что эквивалентно изменению отношения сигнал/шум (SNR) при наличии помех фиксированного уровня. Эксперименты проводились с целью определения максимального и минимального уровней сигнала на входе приемника, которые приводят к экстремальным значениям SNR. Минимальный уровень SNR является пороговым значением, при котором осуществляется решение навигационной задачи с очень грубой точностью.

В нормальных условиях эксплуатации приемника уменьшение SNR до минимального порогового значения является маловероятным случаем. Во-первых, при полете БВС на высоте приемник не подвержен влиянию многолучевости, затенений сигналов и других ухудшающих факторов, поэтому SNR будет достаточно стабильным. Во-вторых, в случае влияния широкополосных или узкополосных помех наблюдается снижение уровней SNR для всех спутников (в зависимости от структуры спутникового приемника), находящихся в решении навигационной задачи. Поэтому необходимо оценивать среднее значение SNR по сигналам от всех навигационных спутников, находящихся в решении.

В качестве примера на рис. 2 представлен график зависимости SNR от уровня входного сигнала для навигационного спутника GPS № 3. Из рис. 2 следует, что уменьшение уровня входного сигнала приводит к уменьшению SNR.

В табл. 1 представлены средние значения SNR видимых созвездий отдельно ГЛОНАСС и GPS, расчет которых проводился по формуле

$$M_{GPS,ГЛОНАСС} = \frac{1}{N_{GPS,ГЛОНАСС}} \sum_{i=1}^{N_{GPS,ГЛОНАСС}} SNR_i , \quad (1)$$

где N – количество видимых спутников наблюдаемой системы; i – порядковый номер видимого НС конкретной системы.

Из таблицы видно, что уменьшение уровня входного сигнала ниже −135 дБмВт не приводит к существенному ухудшению SNR.

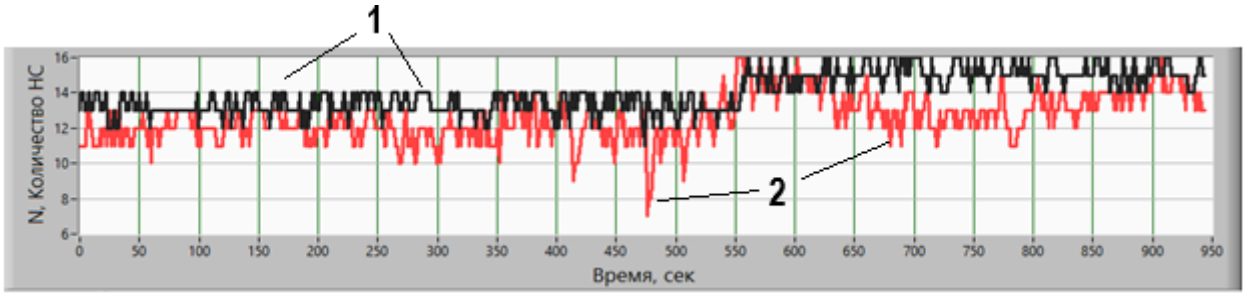
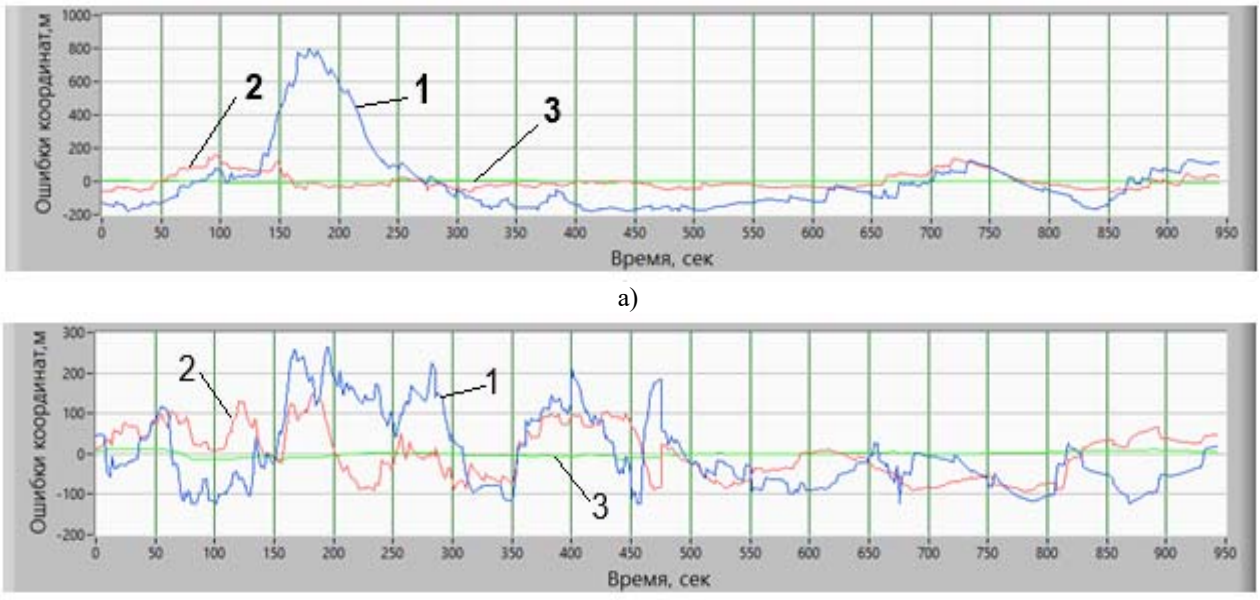


Рис. 3. Количество НС (N), находящихся в решении
Fig. 3. Number (N) of satellites used in solution



а)

б)

Рис. 4. Ошибки измерения координат при решении навигационной задачи по созвездию ГЛОНАСС/GPS с входным уровнем сигнала −140 дБмВт
Fig. 4. Positioning errors in solving a navigation problem with GLONASS/GPS constellation at the input level of −140 dBmW

При максимальном уровне сигнала, равном −100 дБмВт, уровень SNR составляет примерно 50 дБГц для системы GPS и 52 дБГц для системы ГЛОНАСС, что в реальных условиях эксплуатации не наблюдается. Поэтому среднее значение SNR всего видимого созвездия, равное 50 дБГц, можно использовать в качестве верхнего порога, определяющего наличие уводящей помехи.

В случае приема сигналов с критическим уровнем −135 и −140 дБмВт приемник не может обеспечить стабильное слежение за НС, что приводит к включению и выключению из решения навигационной задачи некоторых спутников (рис. 3, кривая 1 – количество НС при уровне входного сигнала −135 дБмВт, кривая 2 – при уровне −140 дБмВт). К таким НС прежде всего относятся те, дальность до которых будет наибольшей (как правило, это горизонтные НС).

Оценки СКО определения координат приемником на интервале времени 950 с составили:

для уровня входного сигнала −135 дБмВт по широте σ_B = 46,8 м, по долготе σ_L = 204,7 м, по высоте σ_H = 3,8 м;

для уровня входного сигнала −140 дБмВт σ_B = 60,7 м, σ_L = 92,6 м, σ_H = 6,3 м;

для уровня входного сигнала −120 дБмВт (уровень в реальных условиях эксплуатации приемника) σ_B = 2,2 м, σ_L = 3,8 м, σ_H = 0,07 м.

На рис. 4 представлены графики ошибок определения координат (широты δB – кривая 1,

долготы δL – кривая 2, высоты δH – кривая 3) для уровня входного сигнала −135 дБмВт (рис. 4, *а*) и −140 дБмВт (рис. 4, *б*). Из рис. 4, *б* видно, что из-за нестабильности горизонтных НС ошибки измерения горизонтальных координат изменяются достаточно существенно.

На основании полученных результатов для минимального уровня сигнала следует выбрать порог, равный 26 дБГц, который является недопустимым уровнем в реальных условиях функционирования приемника GNSS, что позволит определить наличие помех.

Таким образом, для определения наличия помех, сбивающих коррелятор спутникового навигационного приемника, будет использоваться нижний порог, равный 26 дБГц, а в случае уводящей помехи (спуфинга) будет использоваться верхний порог, равный 50 дБГц. Поэтому в качестве критерия определения наличия помех используем соотношение

$$26\ дБГц \leq M_{GPS,ГЛОНАСС,Beidou} \leq 50\ дБГц.$$

Для того чтобы исключить из предложенного критерия влияние снижения уровней SNR от тех НС, которые входят в зону слежения приемника или выходят из нее, необходимо добавить второй критерий. Таким критерием будет сравнение количества НС в решении навигационной задачи в приемнике GNSS с заданным значением. В качестве заданного значения количества НС для каждой навигационной системы выберем 4 спутника, поскольку такое число НС является минимально необходимым для решения навигационной задачи и достаточным при использовании НС от других спутниковых систем при работе приемника GNSS в мультисистемном режиме. Поэтому общий критерий обнаружения воздействия помехи будет следующим:

$$4 \leq N \vee 26\ дБГц \leq M_{GPS,ГЛОНАСС,Beidou} \leq 50\ дБГц. \quad (2)$$

Алгоритм определения наличия помехи

Алгоритм обнаружения наличия помех в навигационных приемниках представлен на рис. 5.

На первом шаге работы алгоритма задаются входные данные с приемника в виде значений SNR для трех систем (SNR_{GPS}, $SNR_{ГЛОНАСС}$, SNR_{Beidou}), количество НС, находящихся в решении (N_{GPS}, $N_{ГЛОНАСС}$, N_{Beidou}), и текущие координаты БВС (B_X, L_X, H_X), а также координаты плана полета БВС (B, L, H), который задается на этапе предполетной подготовки.

На втором шаге производится расчет среднего значения SNR по видимому созвездию для каждой системы в отдельности (SNR_{GPS}, $SNR_{ГЛОНАСС}$, SNR_{Beidou}) согласно выражению (1).

На третьем шаге рассчитанные значения средних SNR по каждой из систем сравниваются с условием (2). В случае невыполнения условия по одной из систем предполагается наличие на входе приемника узкополосной помехи на частоте одной из навигационных систем, поэтому автоматически формируется команда в приемник GNSS по исключению данной спутниковой системы из решения навигационной задачи, что приведет к улучшению точности определения координат и стабильной его работе.

В случае невыполнения условия по всем системам одновременно принимается решение о наличии на входе приемника широкополосной помехи. При этом формируется информационное сообщение оператору БВС о невозможности дальнейшего использования приемника GNSS, а также предлагается использовать ручное управление полетом БВС, что позволит избежать первого этапа влияния спуфинга.

В случае если условие выполняется хотя бы по одной из систем, осуществляется переход на следующий этап проверки.

На четвертом шаге проводится сопоставление выходных координат БВС с координатами полетного задания. Данный этап позволяет обнаружить наличие уводящей помехи, если злоумышленниками не формировалась помеха для обнуления коррелятора приемника GNSS или подмена сигналов НС осуществлена до включения приемника GNSS.

Если условие выполняется, то наличие спуфинга не обнаружено, и алгоритм повторяется с начала с обновленными данными от приемника.

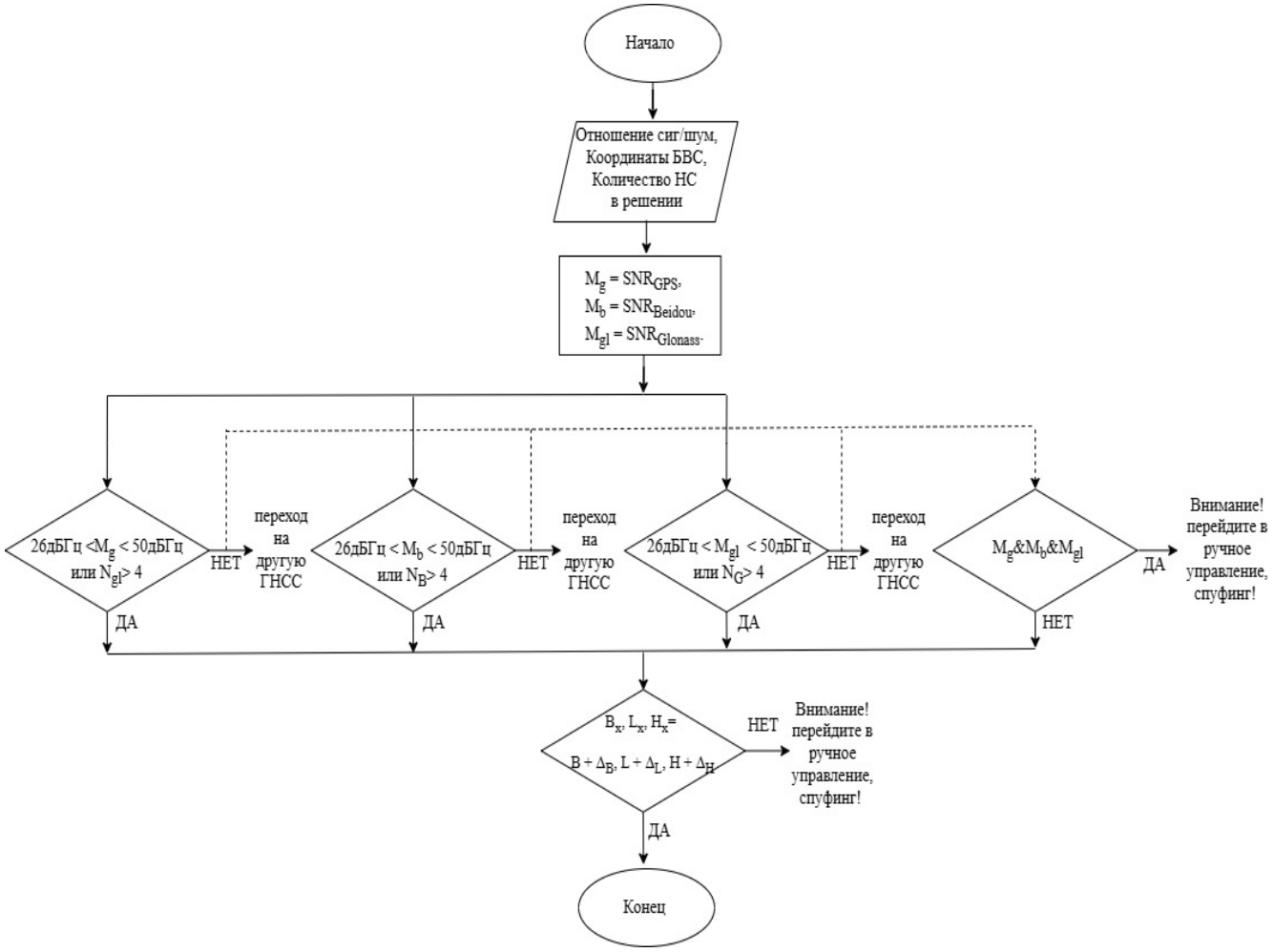


Рис. 5. Алгоритм определения наличия помех
Fig. 5. The algorithm for detecting the interference

Если условие не выполнилось, то формируется автоматическое сообщение пилоту БВС о необходимости перехода на ручное управление БВС, а сам приемник GNSS отключается от бортового контроллера для предотвращения дальнейшего увода БВС по ложной траектории.

Для исключения выполнения данного условия из-за погрешностей позиционирования к каждому значению расчетной координаты из плана полета добавляется некоторая величина (Δ_B, Δ_L и Δ_H). В данной работе Δ_B, Δ_L были заданы 10 м (которые переводились в доли градусов широты и долготы), а значение Δ_H задавалось равным 5 м, что позволяет избежать резкого изменения высоты. Высота полета БВС определяется с помощью приемника GNSS на высотах больше 60 м, на высотах менее 60 м для определения высоты используется баровысотомер с оптическими системами стабилизации.

Таким образом, разработанный алгоритм позволяет обеспечить решение навигационной задачи приемником GNSS на борту БВС при влиянии узкополосной помехи с допустимым уровнем на частоте одной из систем, а также выдать предупреждение оператору, если на входе приемника GNSS присутствует широкополосная помеха или в случае подмены сигналов от НС, в результате которой координаты с выхода приемника начали отличаться от заданных координат маршрута полета.

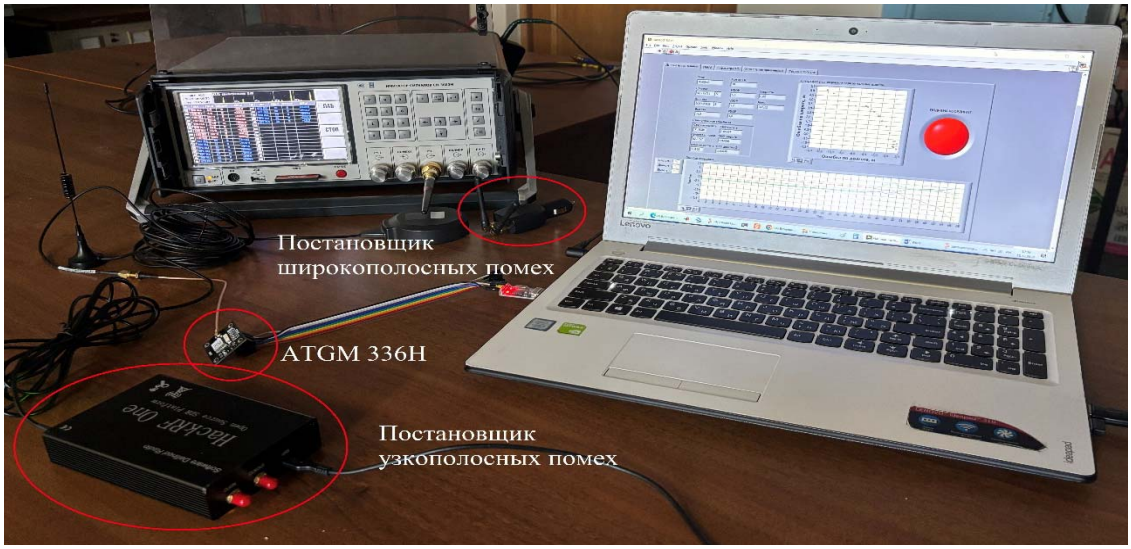


Рис. 6. Стенд для проведения тестирования алгоритма обнаружения помех
Fig. 6. The test bench for testing the algorithm for detecting the interference

Результаты тестирования алгоритма с помощью полунатурного моделирования

На рис. 6 представлен стенд для проведения тестирования алгоритма обнаружения помех. В состав стенда входят:

- имитатор сигналов СН-3803М, формирующий сигналы навигационных спутников систем GPS и ГЛОНАСС согласно заданному сценарию, в котором неподвижный объект находится в точке с нулевыми координатами;
- модуль HackRF One, используемый в качестве постановщика узкополосной помехи с уровнем сигнала 15 дБмВт;
- двухдиапазонный передатчик широкополосной помехи мощностью 1 Вт;
- исследуемый приемный модуль GNSS ATGM336H.

Тестирование разработанного алгоритма проводилось в четыре этапа.

1. Формирование узкополосной помехи на частоте GPS и на частоте первой литеры системы ГЛОНАСС.

2. Формирование сигнала имитатором выше уровня порога, что соответствует подавленному сигналу GNSS подменным сигналом более высокой мощности.

3. Формирование широкополосной помехи.

4. Подмена НС, что привело к движению БВС по ложной траектории.

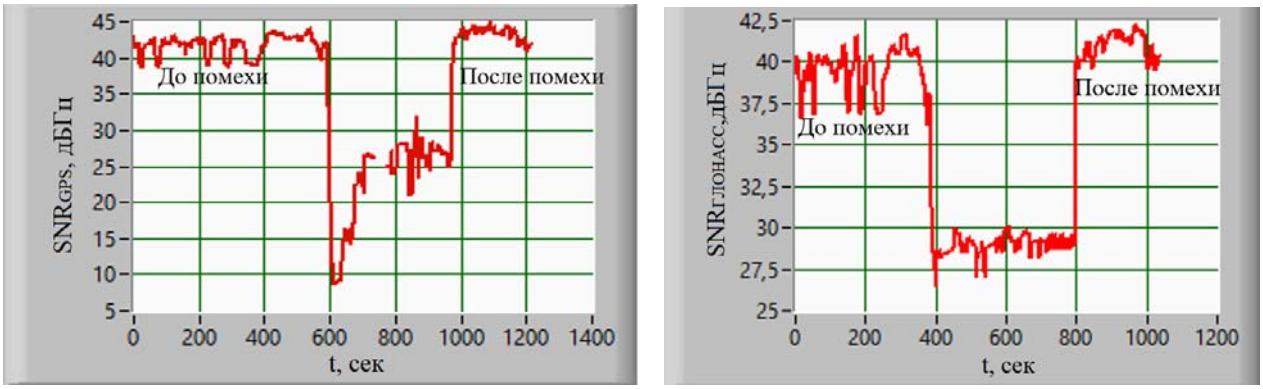
Результаты исследования влияния узкополосной помехи на частоте GPS и на частоте первой литеры системы ГЛОНАСС

С помощью модуля HackRF One ставилась помеха на частоте GPS L1 = 1575,42 МГц мощностью 30 мВт, при этом антенна постановщика помех устанавливалась рядом с антеннами имитатора и приемника.

На рис. 7 представлены графики изменения среднего значения SNR_{GPS} и $SNR_{ГЛОНАСС}$. Из полученных результатов видно, что временны́е отчеты между собой не совпадают, что связано с разным временем поиска и захвата сигналов систем GPS и ГЛОНАСС.

Резкий спад SNR_{GPS} примерно до 8 дБГц (рис. 7, *а*) связан с моментом формирования узкополосной помехи. В течение всего времени действия помехи наблюдается нестабильное слежение за сигналами от НС GPS.

Резкий спад $SNR_{ГЛОНАСС}$ (рис. 7, *б*) связан со структурой модуля ATGM336H, а именно с прохожденим одной из гармоник при преобразовании частот в канале ГЛОНАСС. При этом уровень $SNR_{ГЛОНАСС}$ выше установленного уровня нижнего порога 26 дБГц. Поэтому решение навигационной задачи по системе ГЛОНАСС возможно, и алгоритм формирует команду на отключение сигналов системы GPS.



а б

Рис. 7. Уровни SNR: *а* – SNR_{GPS}, *б* – $SNR_{ГЛОНАСС}$
Fig. 7. SNR levels: *a* – SNR_{GPS}, *b* – $SNR_{GLONASS}$

Рис. 8. Ошибки измерения координат при помехе на частоте GPS
Fig. 8. Positioning errors with interference at the GPS frequency

На рис. 8 представлены погрешности измерения координат модулем ATGM336H (широты δB – кривая 1, долготы δL – кривая 2, высоты δH – кривая 3). На рисунке выделен момент постановки помехи, что привело к росту ошибок определения координат.

После формирования алгоритмом команды на отключение приема сигнала по каналу GPS наблюдается уменьшение ошибок измерения координат, что говорит еще о возможном использовании приемника GNSS, но с большей погрешностью по сравнению с точностью до начала действия помехи.

При постановке узкополосной помехи на частоте 1 602 МГц одной из литер системы ГЛОНАСС наблюдается срыв слежения практически за всеми сигналами от НС ГЛОНАСС.

На рис. 9 представлены графики количества НС N (рис. 9, *а, в*), находящихся в решении для каждой системы, и средних значений SNR (рис. 9, *б, г*). Отмеченные моменты на графиках количества НС в решении и $SNR_{ГЛОНАСС}$ (рис. 9, *а, б*) связаны с кратковременным отключением помехи, что не повлияло на точность измерения координат в целом. Значительное ухудшение SNR_{GPS} не наблюдается, поэтому приемник работает с хорошей точностью определения координат (рис. 10, где кривая 1 – ошибка δB, кривая 2 – ошибка δL, кривая 3 – ошибка δH).

Результаты исследования влияния подменного сигнала высокого уровня

Установка высокого уровня сигнала имитатором (выше уровня реального сигнала GNSS) привела к росту SNR_{GPS} и $SNR_{ГЛОНАСС}$

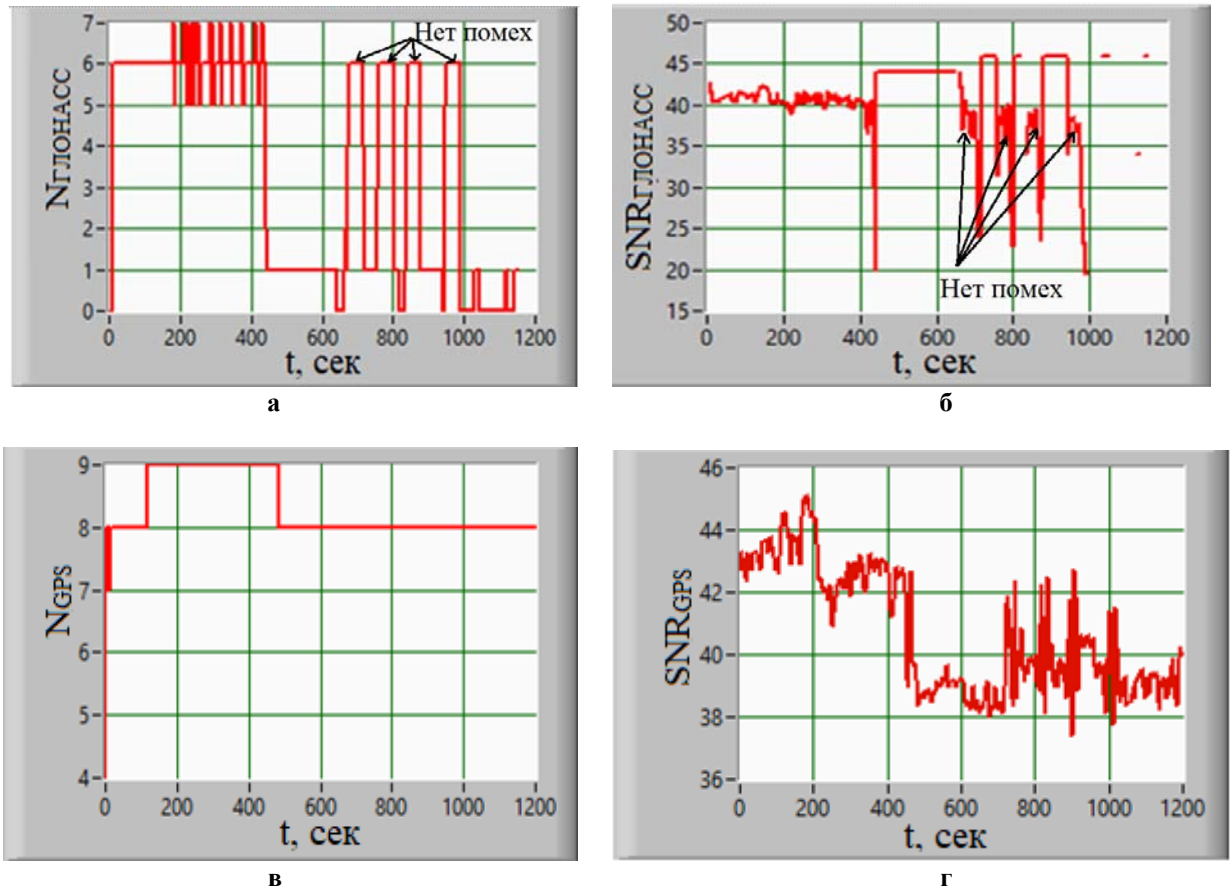
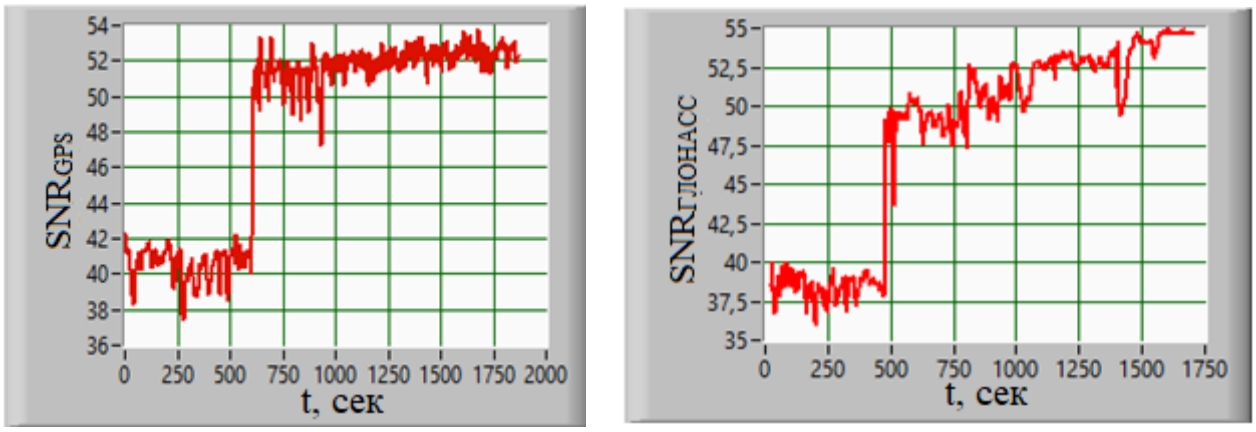


Рис. 9. Результаты эксперимента: *а* – количество НС ГЛОНАСС в решении; *б* – $SNR_{ГЛОНАСС}$; *в* – количество НС GPS в решении; *г* – SNR_{GPS}
Fig. 9. The results of the experiment: *а* – number of GLONASS satellites ised in solution; *б* – $SNR_{GLONASSC}$; *в* – number of GPS satellites ised in solution; *г* – SNR_{GPS}

Рис. 10. Погрешности измерения координат при помехе на частоте ГЛОНАСС
Fig. 10. Positioning errors with interference at the GLONASS frequency

и превышению установленного порога 50 дБГц (рис. 11, *а, б*), поэтому алгоритм формирует соответствующее сообщение. Такое событие отображается на интерфейсе программного модуля, разработанного в среде LabView (рис. 12). При практической реализации данное сообщение должно поступать в полетный контроллер БВС и далее по линии контроля и управления С2 на пульт оператора БВС.



а б

Рис. 11. Результаты эксперимента: *а* – SNR_{GPS}; *б* – $SNR_{ГЛОНАСС}$
Fig. 11. The results of the experiment: *а* – SNR_{GPS}; *б* – $SNR_{GLONASS}$

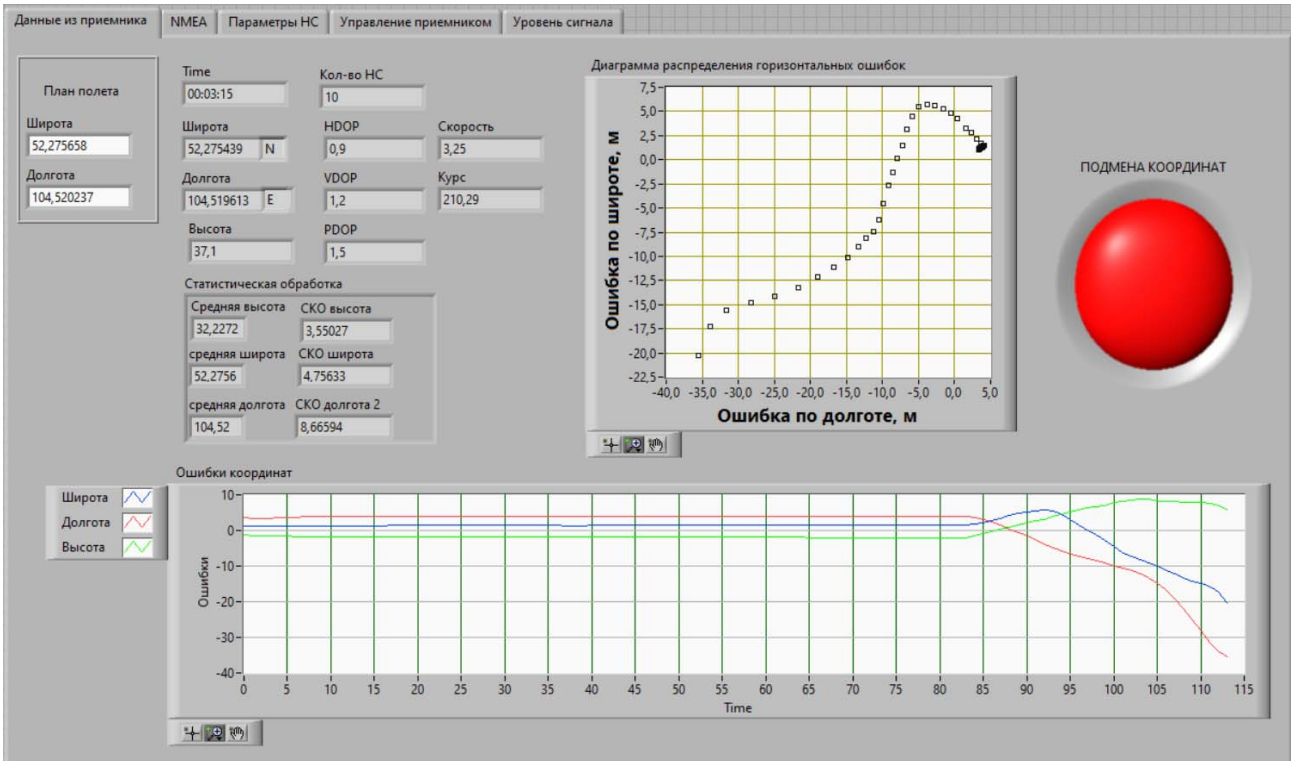
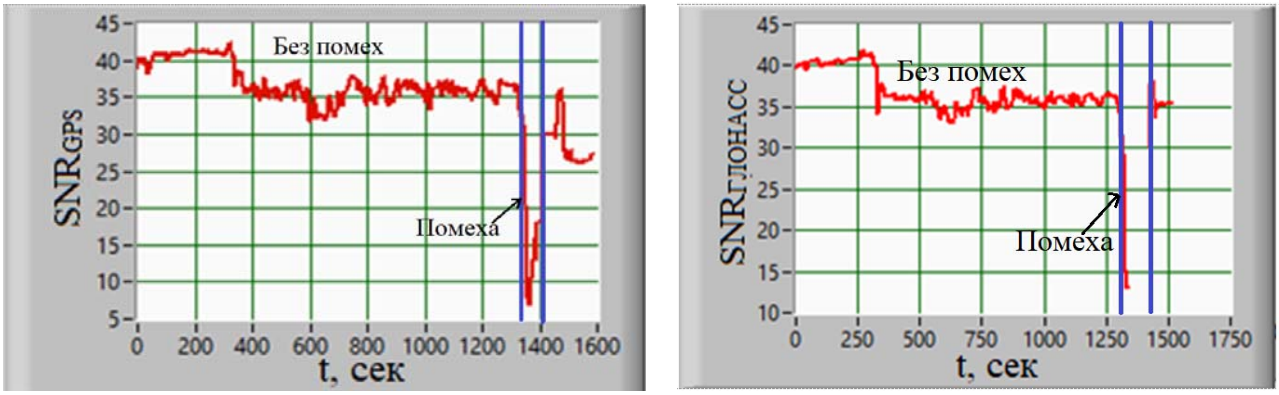


Рис. 12. Интерфейс программного модуля
Fig. 12. The interface of the programming module

Результаты исследования влияния широкополосной помехи

Даже кратковременное включение широкополосной мощной помехи приводит к полному подавлению сигналов спутников GPS и ГЛОНАСС. На рис. 13 показан момент включения помехового сигнала и снижение уровня SNR_{GPS} и $SNR_{ГЛОНАСС}$ ниже порогового значения. В этом случае координаты от приемника GNSS являются недоступными, поэтому отсутствует навигация и стабилизация БВС. В этом случае алгоритм формирует сообщение оператору БВС о необходимости перехода на ручное управление БВС.



а б

Рис. 13. Результаты эксперимента: *а* – SNR_{GPS}; *б* – $SNR_{ГЛОНАСС}$
Fig. 13. The results of the experiment: *а* – SNR_{GPS}; *б* – $SNR_{GLONASS}$

Результаты исследования действия уводящей помехи, приводящей к смене траектории БВС

На этом этапе внешние постановщики помех не использовались. Предполагается, что на вход приемника поступают ложные сигналы от системы GNSS и это приведет к уводу БВС с заданного маршрута полета.

Для тестирования разработанного алгоритма работы имитатора СН-3803М был написан сценарий, при котором первые 2 минуты БВС находится в точке с координатами B = 52,2756°, L = 104,520237°, H = 30 м, которые совпадают с планом полета, а затем имитатор создает сигналы, имитирующие движение БВС с постоянной скоростью и курсом, равным 0° (сигналы спуфинга), что соответствует движению по ложной траектории.

При наличии спуфинга текущие координаты БВС не совпадают с координатами плана полета и загорается сигнализатор подмены координат (рис. 12).

В реальных ситуациях при выполнении данного условия будет сформировано сообщение пилоту о принятии управления на себя и данные с приемника GNSS не будут использоваться в навигационном контроллере БВС, что предотвратит увод БВС по ложной траектории.

Заключение

В настоящей работе представлена методика обнаружения воздействия узкополосного и широкополосного помеховых сигналов, а также спуфингового сигнала на приемник GNSS. Для реального приемного модуля ATGM336H разработан интерфейс программы обработки данных с дальнейшим их анализом для идентификации типа помехи. Интерфейс программы на основе разработанного алгоритма позволяет формировать сообщения пилоту БВС в случае невозможности использования спутникового приемника и выбирать спутниковую систему в зависимости от частоты установки узкополосной системы. Таким образом повышается помехоустойчивость приемника GNSS, а также повышается уровень ситуационной осведомленности оператора БВС в условиях сложной помеховой обстановки.

Список литературы

1. **Толстиков А.С., Ушаков А.Е.** Противодействие спуфингу и повышение помехоустойчивости аппаратуры потребителя глобальных навигационных спутниковых систем // Интерэкспо Гео-Сибирь. 2018. № 9. С. 319–327.

2. **Арефьев Р.О., Скрыпник О.Н., Межетов М.А.** Исследование помехоустойчивости мультисистемного GNSS приемника //

Crede Experto: транспорт, общество, образование, язык. 2023. № 2. С. 28–43. DOI: 10.51955/2312-1327_2023_2_28

3. Grant A. GPS jamming and the impact on maritime navigation / A. Grant, P. Williams, N. Ward, S. Baske // The Journal of Navigation. 2009. Vol. 62, no. 2. Pp. 173–187. DOI: 10.1017/S0373463308005213

4. Hofmann-Wellenhof B., Lichtenegger H., Wasle E. GNSS-global navigation satellite systems: GPS, GLONASS, Galileo, and more. New York: Springer Wien, 2008. 547 p.

5. Kaplan E., Hegarty C. Understanding GPS: principles and applications. 2nd ed. Artech house on Demand, 2005. 726 p.

6. Соловьев Ю.А. Системы спутниковой навигации. М.: Эко-Трендз, 2000. 270 с.

7. Вознюк В.В., Маслаков П.А., Фомин А.В. Исследование помехоустойчивости аппаратуры потребителей глобальной навигационной спутниковой системы GPS на основе технологии программного приема // Труды Военно-космической академии имени А.Ф. Можайского. 2016. № 650. С. 33–40.

8. Glomsvoll O., Bonenberg L.K. GNSS jamming resilience for close to shore navigation in the Northern Sea // The Journal of Navigation. 2017. Vol. 70, no. 1. Pp. 33–48. DOI: 10.1017/S0373463316000473

9. Glomsvoll O. Jamming of GPS & GLONASS signals. Department of Civil Engineering, Nottingham Geospatial Institute, 2014. 80 p.

10. Meng L. A survey of GNSS spoofing and anti-spoofing technology / L. Meng, L. Yang, W. Yang, L. Zhang [Электронный ресурс] // Remote sensing. 2022. Vol. 14, iss. 19. ID: 4826. DOI: 10.3390/rs14194826 (дата обращения: 23.02.2025).

11. Psiaki M.L., Humphreys T.E. GNSS spoofing and detection // Proceedings of the IEEE. 2016. Vol. 104, no. 6. Pp. 1258–1270. DOI: 10.1109/JPROC.2016.2526658

12. Junzhi L. Research progress of GNSS spoofing and spoofing detection technology / L. Junzhi, L. Wanqing, F. Qixiang, L. Beidian // 2019 IEEE 19th International Conference on Communication Technology (ICCT). China, Xi'an, 2019. Pp. 1360–1369. DOI: 10.1109/ICCT46805.2019.8947107

13. Radoš K., Brkić M., Begušić D. Recent advances on jamming and spoofing detection in GNSS [Электронный ресурс] // Sensors. 2024. Vol. 24, iss. 13. ID: 4210. DOI: 10.3390/s24134210 (дата обращения: 23.02.2025).

14. Мельниченко С. Спуфинг – новые высоты [Электронный ресурс] // AviaSafety.ru 2024. URL: https://aviasafety.ru/47840/ (дата обращения: 23.02.2025).

15. Broumandan A., Siddakatte R., Lachapelle G. An approach to detect GNSS spoofing // IEEE Aerospace and Electronic Systems Magazine. 2017. Vol. 32, no. 8. Pp. 64–75. DOI: 10.1109/MAES.2017.160190

16. Liu Y. Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system / Y. Liu, S. Li, Q. Fu, Z. Liu [Электронный ресурс] // Sensors. 2018. Vol. 18, iss. 5. ID: 1433. DOI: 10.3390/s18051433 (дата обращения: 23.02.2025).

17. Lee D.K., Miralles D., Akos D. et al. Detection of GNSS spoofing using NMEA messages // 2020 European Navigation Conference (ENC). IEEE, Germany, Dresden, 2020. Pp. 1–10. DOI: 10.23919/ENC48637.2020.9317470

18. Spravil J. Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring / J. Spravil, C. Hemminghaus, M. von Rechenberg, E. Padilla, J. Bauer [Электронный ресурс] // Journal of Marine Science and Engineering. 2023. Vol. 11, iss. 5. ID: 928. DOI: 10.3390/jmse11050928 (дата обращения: 23.02.2025).

19. Перов А.И., Харисов В.Н. ГЛОНАСС. Принципы построения и функционирования. 4-е изд., перераб. и доп. М.: Радиотехника, 2010. 801 с.

References

1. Tolstikov, A.S, Ushakov, A.E. (2018). Countering spoofing and improving the noise immunity of coordinate-time definitions of GNSS technologies. *Interekspo Geo-Sibir*, no. 9, pp. 319–327. (in Russian)

2. Arefyev, R.O., Skrypnik, O.N., Mezhetov, M.A. (2023). The research of the immunity of the multisystem GNSS receiver.

Crede Experto: transport, society, education, language, no. 2, pp. 28–43. DOI: 10.51955/2312-1327_2023_2_28 (in Russian)

3. Grant, A., Williams, P., Ward, N., Baske, S. (2009). GPS jamming and the impact on maritime navigation. *The Journal of Navigation*, vol. 62, no. 2, pp. 173–187. DOI: 10.1017/S0373463308005213

4. Hofmann-Wellenhof, B., Lichtenegger, H., Wasle, E. (2008). GNSS-global navigation satellite systems: GPS, GLONASS, Galileo, and more. Springer Wien New York, 547 p.

5. Kaplan, E., Hegarty, C. (2005). Understanding GPS: principles and applications. 2nd ed. Artech house on Demand, 726 p.

6. Soloviev, Yu.A. (2000). Satellite navigation systems. Moscow: Eko-Trendz, 270 p. (in Russian)

7. Voznuk, V.V., Maslakov, P.A., Fomin, A.V. (2016). The research of the interference immunity of users' GPS equipment based on the SDR technology. *Trudy Voenno-kosmicheskoy akademii imeni A.F. Mozhayskogo*, no. 650, pp. 33–40. (in Russian)

8. Glomsvoll, O., Bonenberg, L.K. (2017). GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation*, vol. 70, no. 1, pp. 33–48. DOI: 10.1017/S0373463316000473

9. Glomsvoll, O. (2014). Jamming of GPS & GLONASS signals. Department of Civil Engineering, Nottingham Geospatial Institute, 80 p.

10. Meng, L., Yang, L., Yang, W., Zhang, L. (2022). A survey of GNSS spoofing and anti-spoofing technology. *Remote sensing*, vol. 14, issue 19, ID: 4826. DOI: 10.3390/rs14194826 (accessed: 23.02.2025).

11. Psiaki, M.L., Humphreys, T.E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270. DOI: 10.1109/JPROC.2016.2526658

12. Junzhi, L., Wanqing, L., Qixiang, F., Beidian, L. (2019). Research progress of GNSS spoofing and spoofing detection technology. *In: 2019 IEEE 19th international conference on communication technology (ICCT)*. Xi'an, China, pp. 1360–1369. DOI: 10.1109/ICCT46805.2019.8947107

13. Radoš, K., Brkić, M., Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. *Sensors*, vol. 24, issue 13, ID: 4210. DOI: 10.3390/s24134210 (accessed: 23.02.2025).

14. Melnichenko, S. (2024). Spoofing – New Heights. *AviaSafety.ru*. 2024. Available at: https://aviasafety.ru/47840/ (accessed: 23.02.2025). (in Russian)

15. Broumandan, A., Siddakatte, R., Lachapelle, G. (2017). An approach to detect GNSS spoofing. *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 8, pp. 64–75. DOI: 10.1109/MAES.2017.160190

16. Liu, Y., Li, S., Fu, Q., Liu, Z. (2018). Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system. *Sensors*, vol. 18, issue 5, ID: 1433. DOI: 10.3390/s18051433 (accessed: 23.02.2025).

17. Lee, D.K., Miralles, D., Akos, D. et al. (2020). Detection of GNSS spoofing using NMEA messages. *In: 2020 European Navigation Conference (ENC)*, IEEE, Germany, Dresden, pp. 1–10. DOI: 10.23919/ENC48637.2020.9317470

18. Spravil, J., Hemminghaus, C., von Rechenberg, M., Padilla, E., Bauer, J. (2023). Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. *Journal of Marine Science and Engineering*, vol. 11, issue 5. ID: 928. DOI: 10.3390/jmse11050928 (accessed: 23.02.2025).

19. Perov, A.I., Kharisov, V.N. (2010). GLONASS. Principles of construction and operation. 4th ed., revised and enlarged. Moscow: Radiotekhnika, 801 p. (in Russian)

Сведения об авторах

Арефьев Роман Олегович, кандидат технических наук, доцент, доцент кафедры авиационного радиоэлектронного оборудования Иркутского филиала МГТУ ГА, aqua160905@mail.ru.

Арефьева Наталья Геннадьевна, кандидат технических наук, доцент, доцент кафедры авиационного радиоэлектронного оборудования Иркутского филиала МГТУ ГА, n_astrahanceva_awesome@mail.ru.

Скрыпник Олег Николаевич, доктор технических наук, профессор, профессор кафедры организации движения и обеспечения безопасности на воздушном транспорте Белорусской государственной академии авиации, skripnikon@yandex.ru.

Information about the authors

Roman O. Arefyev, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Aviation Radioelectronic Equipment Chair, Irkutsk Branch of the Moscow State Technical University of Civil Aviation, aqua160905@mail.ru.

Natalya G. Arefyeva, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Aviation Radioelectronic Equipment Chair, Irkutsk Branch of the Moscow State Technical University of Civil Aviation, n_astrahanceva_awesome@mail.ru.

Oleg N. Skrypnik, Doctor of Technical Sciences, Professor, Professor of the Organization of Traffic and Ensuring Safety in Air Transport, Belarusian State Aviation Academy, skripnikon@yandex.ru.

Поступила в редакцию	27.06.2025	Received	27.06.2025
Одобрена после рецензирования	01.08.2025	Approved after reviewing	01.08.2025
Принята в печать	20.11.2025	Accepted for publication	20.11.2025